UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/510,403	02/21/2007	Richard Critten	18305-002US1	6296

20985 7590 03/21/2008
FISH & RICHARDSON, PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
KAPLAN, BENJAMIN A	
ART UNIT	PAPER NUMBER
2139	
MAIL DATE	DELIVERY MODE
03/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/510,403	**Applicant(s)** CRITTEN ET AL.	
	Examiner BENJAMIN A. KAPLAN	**Art Unit** 2139	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 February 2007*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-50* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 October 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *11/18/2004 & 04/17/2007*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. Claims 1-50 are pending.

Information Disclosure Statement

2. In the information disclosure statement filed 11/18/2004 the reference under Other Documents designated by the ID of (AQ) fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent listed that is not in the English language. It has been placed in the application file, but the information referred to therein has not been considered.

Claim Objections

3. Claim 35 is objected to because of the following informality: There is a “15" in the middle of the last line of claim 35. Appropriate correction is required.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 29-50 are rejected as being non-statutory because they recite a computer program per se representing functional descriptive material without a memory and a processor.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claims 1-5, 12, 15-22, 25-32, 35-47 & 49 are rejected under 35 U.S.C. 102(b) as being anticipated by WIPO Publication WO 01/44949 A2.

7. The publication is applied by way of the English translation provided by the Canadian national entry of this application Canadian Intellectual Property Office Publication CA 2395381 A1 (Freedman)

<u>As Per Claim 1:</u> Freedman teaches:

- A method of authenticating a computer user comprising

(Column 1, Lines 6-14, "Access to many computer programs, such as operating systems and application programs, for example for electronic mail, e-commerce, home banking, etc, requires authentication of the user vis-à-vis the program concerned. When a user starts a program requiring authentication on a terminal such as a personal computer, the program generally displays on the screen of the terminal a dialog box including two fields, one for entering the login name of the user and the other for entering their password. These credentials are specific to the user and to the program concerned and the user enters them via the keyboard of the terminal.").

- unlocking a secure media using a user entered identification

(Column 5, Lines 24-27, "said personal security device includes means for comparing a stored secret code with a secret code entered by the user via said interface means and said access control means are rendered operational in response to a match between said secret codes").

- retrieving authentication credentials for the user from the secure media, the authentication credentials including a password, verifying the authentication credentials and, on successful verification, authenticating the user

(Column 7, Lines 16-20, "In a system according to the invention, the various credentials, and in particular the passwords PWD1, PWD2, PWD3, PWD4 for the applications 1 to 4, are supplied to the personal computer 1 by the personal security device 5. As previously indicated, the credentials, such as the passwords, can be static or dynamic.").

As Per Claim 2: The rejection of Claim 1 is incorporated and further Freedman teaches:

- the retrieval of authentication credentials comprises retrieving the credentials from a vault

(Column 3, Lines 16-23, "The data processing system according to the invention does not require manual entry by the user of their credentials, which are automatically transferred by means of the pointing device of the personal safety device to the software to which the user requires access. Because the user's personal security device, whether of the hardware type (smart card, token) or the software type, can store strong (long and complex) passwords, the data processing system according to the invention significantly improves security for access to one or more programs.").

As Per Claim 3: The rejection of Claim 2 is incorporated and further Freedman teaches:

- the vault is located on the secure media

(Column 3, Lines 16-23, as seen in the rejection of claim 2).

As Per Claim 4: The rejection of Claim 3 is incorporated and further Freedman teaches:

- the secure media is a smart card

(Column 3, Lines 16-23, as seen in the rejection of claim 2).

<u>As Per Claim 5:</u> The rejection of Claim 2 is incorporated and further Freedman teaches:

- the vault is a secure file

(Column 3, Lines 16-23, as seen in the rejection of claim 2).

Software file or file on the smart card.

<u>As Per Claim 12:</u> The rejection of Claim 1 is incorporated and further Freedman teaches:

- the authentication permits user access to a computer system, wherein secure media is unlocked by the system graphical identification and authentication module (GINA) an the authentication credentials are retrieved by the GINA from the secure media and passed to the computer operating system for verification as part of the operating system logon procedure

(Column 8 Line 26 - Column 9 Line 7, “The passwords PWDI, PWD2, PWD3, PWD4 supplied by the smart card 5 are associated with the features of the window in which the passwords are entered, in this instance the class and the attributes of the window.

The process illustrated by the dashed line arrow F in Figure 1 for entering the password supplied by the smart card 5 into the required window of one of the applications 1 to 4 will be explained further with reference also to Figures 2A and 2B.

The process is based on the use of graphical user interface "Drag-and-Drop" type functions. The Drag-and-Drop technique is a graphical user interface (GUI) technique for transferring data between two applications. The mouse of the personal computer is used to extract data from one application and insert it into another application. For example, it is possible to select a block of text in a word processing program. Moving the cursor onto the selected block of text with the mouse and holding down the mouse button while moving the mouse to shift the cursor to the required location in another application inserts the text into that other application simply by releasing the mouse button. The Drag-and-Drop technique therefore presupposes a source, namely an application from which data is extracted, and a target, into which the data is inserted.").

As Per Claim 15: The rejection of Claim 1 is incorporated and further Freedman teaches:

- the authentication permits user access to an application running on a computer system comprising generating scripts corresponding to application authentication requests

(Column 4 Line 33 – Column 5 Line 9, "In a variant of the invention, if the system includes a plurality of programs and a plurality of separate credentials controlling access to respective programs, each of the credentials is associated in said supply means with data identifying the corresponding program, and said access control means further include second means for identifying a program whose destination window is displayed on said screen, and second comparator means for comparing the identity of said program detected with said identification data stored in said supply means, said application means being adapted to command application in said destination window of credentials present in said supply means and whose associated identification data corresponds to the identity of said detected program. In this embodiment the authentication process is automated in the sense that the user does not have to choose the credentials assigned to the program to which access is required, provided that the credentials are available in the personal security device.").

The associations and comparator operations are the scripts.

__**As Per Claim 16:**__ The rejection of Claim 15 is incorporated and further Freedman teaches:

- the script generation comprises navigating the application to an authentication screen, selecting the authentication screen, generating a script corresponding to the application screen, testing the generated script and saving the script

(Column 4 Line 33 – Column 5 Line 9, as seen in the rejection of claim 15).

(Column 10 Lines 26–37, "It must be understood that the applications 1, 2, 3 and 4 are not modified in any way and are standard applications. Consequently, the resident access control program LPA is substituted for entry of the password via the keyboard by the user. Various solutions for this are available to the skilled person. One solution is to simulate the pressing of the keyboard keys and to send to the destination window a message equivalent to that generated by the keyboard. With this solution, the password is transmitted character by character to the destination window. Another solution would be to use the cut/paste function offered by modern operating systems (OS): the password is copied onto the clipboard by the program LPA which then simulates pasting into the target application by sending it a message equivalent to the paste instruction").

Also see (Column 12 Line 17 through Column 13 Line 37).

As Per Claim 17: The rejection of Claim 15 is incorporated and further Freedman teaches:

- distributing the script to one or more users of the application to which it relates

The scripts have been distributed as they are available to the user.

As Per Claim 18: The rejection of Claim 17 is incorporated and further Freedman teaches:

- loading the script at a computer to which the script has been distributed

As the scripts are being used they have been loaded to provide for that usage their of.

As Per Claim 19: The rejection of Claim 15 is incorporated and further Freedman teaches:

- learning user credentials for the application, the user credentials including a password

(Column 13 Lines 30-37, "If the result of the test in step 121 is negative, the user is prompted in step 124 to enter the required password (static password) manually via the keyboard of their personal computer. In step 125 the password, the application identification data and the characteristics of the detected window acquired in steps 117 and 120 are transmitted to the smart card 5, which stores them. The next step of the subroutine is then step 122 which inserts the password entered at the keyboard by the user and stored in the smart card 5 into the destination window.").

As Per Claim 20: The rejection of Claim 19 is incorporated and further Freedman teaches:

- the learning of user credentials comprises running the generated script, detecting an application authentication screen, querying the secure media for authentication credentials for the application, reading authentication credentials submitted by the user if no credentials are found for the application on the secure media, retrieving the submitted credentials from the screen and, on authentication of the end user, saving the credentials at the secure media

(Column 12 Line 17 - Column 13 Line 37, “The following description with reference to Figures 3 to 6 covers a second embodiment in which the user does not need to select the appropriate password, because it is selected automatically by the access control program LPA.

Figure 3 shows the overall way in which the mouse 6 controls the access control program LPA. The process starts with step 100 in which the left-hand mouse button 6a is pressed when the cursor 9 is on top of the icon 7. Step 101 corresponds to capture of the status of the mouse and step 102 to waiting for events that can be generated by the mouse, for example moving the mouse or releasing the left-hand mouse button.

If the event detected is movement of the mouse, the next step is step 103 corresponding to the subroutine whose flowchart is shown in Figure 4.

If the event detected by the access control software concerns the left-hand mouse button, the next step is step 104 corresponding to the subroutine whose flowchart is shown in Figure 5. Step 105 is the last step of the main program.

The Figure 4 subroutine starts in step 106 with detection of movement of the mouse. In step 107 the position of the mouse is acquired. In step 108 the window under the cursor 9 is sought. Step 109 corresponds to the acquisition of characteristic data of the window under the cursor, in particular its class.

Step 110 determines if the class of the window under the cursor corresponds to a window class stored in the smart card 5. If not, the graphical representation of the cursor 9 is modified in step 11 1 to advise the user that at this stage the function for entering the password PWD is inhibited, i.e. that releasing the left-hand mouse button

6a will have no effect. The next step of the subroutine is then the end step 112. However, the Figure 4 subroutine is repeated for as long as the mouse 6 is moving, as is clear from the Figure 3 flowchart.

If the result of the test in step 110 is positive, i.e. if the window under the cursor is of a class contained in the memory of the smart card 5, step 113 modifies the graphical appearance of the cursor (which reverts to the arrow shape that it has when it reaches the window 8 in Figure 2), advising the user that insertion of the password PWD is then authorized.

If the event detected in step 102 in Figure 3 is releasing the left-hand mouse button, the subroutine 104 shown by the Figure 5 flowchart is executed.

Step 114 in Figure 5 corresponds to detecting release of the left-hand mouse button. The position of the mouse is acquired in step 115 and the window under the cursor is sought in step 116. Characteristic data of that window, in particular its class, is acquired in step 117.

Step 118 applies a test to determine if the window under the cursor 9 belongs to a class stored in the smart card 5. If not, the subroutine terminates in step 119.

If it does, the application to which the window belongs is determined in step 120. Step 121 applies a test to determine if the identified application corresponds to an application whose identification data is contained in the smart card 5. If it does, the password in the smart card 5 associated with the identified application is inserted in the window in which the cursor is then located, after which the subroutine terminates in step 123.

If the result of the test in step 121 is negative, the user is prompted in step 124 to enter the required password (static password) manually via the keyboard of their personal computer. In step 125 the password, the application identification data and the characteristics of the detected window acquired in steps 117 and 120 are transmitted to the smart card 5, which stores them. The next step of the subroutine is then step 122 which inserts the password entered at the keyboard by the user and stored in the smart card 5 into the destination window.").

<u>As Per Claim 21:</u> The rejection of Claim 20 is incorporated and further Freedman teaches:

- replaying the stored authentication credentials on subsequent attempts to open the application by the user

As seen in the rejection of claim 20 if the credential is absent it is stored when entered making it present for being replayed on subsequent access attempts.

<u>As Per Claim 22:</u> The rejection of Claim 21 is incorporated and further Freedman teaches:

- the replaying of user credentials comprises detecting the application authentication screen, retrieving the authentication credentials from the secure

media, populating the authentication screen with the authentication credentials and submitting the authentication screen to the application

(Column 12 Line 17 through Column 13 Line 37, as seen in the rejection of claim 20.)

<u>As Per Claim 25:</u> The rejection of Claim 15 is incorporated and further Freedman teaches:

- displaying an application authentication screen to the user when authentication credentials retrieved from the secure media are rejected by the application, receiving correct authentication credentials from the user, submitting the authentication screen with the correct authentication credentials to the application, and on authentication, storing the correct credentials in the secure media

(Column 12 Line 17 - Column 13 Line 37, "The following description with reference to Figures 3 to 6 covers a second embodiment in which the user does not need to select the appropriate password, because it is selected automatically by the access control program LPA.

Figure 3 shows the overall way in which the mouse 6 controls the access control program LPA. The process starts with step 100 in which the left-hand mouse button 6a is pressed when the cursor 9 is on top of the icon 7. Step 101 corresponds to capture of the status of the mouse and step 102 to waiting for events that can be generated by the mouse, for example moving the mouse or releasing the left-hand mouse button.

If the event detected is movement of the mouse, the next step is step 103 corresponding to the subroutine whose flowchart is shown in Figure 4.

If the event detected by the access control software concerns the left-hand mouse button, the next step is step 104 corresponding to the subroutine whose flowchart is shown in Figure 5. Step 105 is the last step of the main program.

The Figure 4 subroutine starts in step 106 with detection of movement of the mouse. In step 107 the position of the mouse is acquired. In step 108 the window under the cursor 9 is sought. Step 109 corresponds to the acquisition of characteristic data of the window under the cursor, in particular its class.

Step 110 determines if the class of the window under the cursor corresponds to a window class stored in the smart card 5. If not, the graphical representation of the cursor 9 is modified in step 11 1 to advise the user that at this stage the function for entering the password PWD is inhibited, i.e. that releasing the left-hand mouse button 6a will have no effect. The next step of the subroutine is then the end step 112. However, the Figure 4 subroutine is repeated for as long as the mouse 6 is moving, as is clear from the Figure 3 flowchart.

If the result of the test in step 110 is positive, i.e. if the window under the cursor is of a class contained in the memory of the smart card 5, step 113 modifies the graphical appearance of the cursor (which reverts to the arrow shape that it has when it reaches the window 8 in Figure 2), advising the user that insertion of the password PWD is then authorized.

If the event detected in step 102 in Figure 3 is releasing the left-hand mouse button, the subroutine 104 shown by the Figure 5 flowchart is executed.

Step 114 in Figure 5 corresponds to detecting release of the left-hand mouse button. The position of the mouse is acquired in step 115 and the window under the cursor is sought in step 116. Characteristic data of that window, in particular its class, is acquired in step 117.

Step 118 applies a test to determine if the window under the cursor 9 belongs to a class stored in the smart card 5. If not, the subroutine terminates in step 119.

If it does, the application to which the window belongs is determined in step 120. Step 121 applies a test to determine if the identified application corresponds to an application whose identification data is contained in the smart card 5. If it does, the password in the smart card 5 associated with the identified application is inserted in the window in which the cursor is then located, after which the subroutine terminates in step 123.

If the result of the test in step 121 is negative, the user is prompted in step 124 to enter the required password (static password) manually via the keyboard of their personal computer. In step 125 the password, the application identification data and the characteristics of the detected window acquired in steps 117 and 120 are transmitted to the smart card 5, which stores them. The next step of the subroutine is then step 122 which inserts the password entered at the keyboard by the user and stored in the smart card 5 into the destination window.").

As Per Claim 26: The rejection of Claim 25 is incorporated and further the limitations of claim 26 have already been covered in the rejection of claim 25.

As Per Claim 27: Claim 27 is substantially a restatement of the method of claim 1 as a computer readable storage medium with code and is rejected under substantially the same reasoning.

As Per Claim 28: Claim 28 is substantially a restatement of the method of claim 1 as a computer or computer network and is rejected under substantially the same reasoning.

As Per Claim 29: Claim 29 is substantially a restatement of the method of claim 1 as an apparatus and is rejected under substantially the same reasoning.

As Per Claim 30: The rejection of claim 29 is incorporated and further Claim 30 is substantially a restatement of the method of claim 3 as an apparatus and is rejected under substantially the same reasoning.

As Per Claim 31: The rejection of claim 30 is incorporated and further Claim 31 is substantially a restatement of the method of claim 4 as an apparatus and is rejected under substantially the same reasoning. Using a smart card intently includes using a smart card reader.

<u>**As Per Claim 32:**</u> The rejection of claim 30 is incorporated and further Claim 32 is substantially a restatement of the method of claim 5 as an apparatus and is rejected under substantially the same reasoning.

<u>**As Per Claim 35:**</u> The rejection of claim 29 is incorporated and further Freedman teaches:

- the authentication permits user access to a computer system, and the means for unlocking the secure media comprises a Graphical Identification and Authentication Module (GINA) arranged to retrieve authentication credentials from the secure media and pass them to the operating system of the computer system for verification as part of the operating 15 system logon procedure

(Column 12 Line 17 - Column 13 Line 37, "The following description with reference to Figures 3 to 6 covers a second embodiment in which the user does not need to select the appropriate password, because it is selected automatically by the access control program LPA.

Figure 3 shows the overall way in which the mouse 6 controls the access control program LPA. The process starts with step 100 in which the left-hand mouse button 6a is pressed when the cursor 9 is on top of the icon 7. Step 101 corresponds to capture of the status of the mouse and step 102 to waiting for events that can be generated by the mouse, for example moving the mouse or releasing the left-hand mouse button.

If the event detected is movement of the mouse, the next step is step 103 corresponding to the subroutine whose flowchart is shown in Figure 4.

If the event detected by the access control software concerns the left-hand mouse button, the next step is step 104 corresponding to the subroutine whose flowchart is shown in Figure 5. Step 105 is the last step of the main program.

The Figure 4 subroutine starts in step 106 with detection of movement of the mouse. In step 107 the position of the mouse is acquired. In step 108 the window under the cursor 9 is sought. Step 109 corresponds to the acquisition of characteristic data of the window under the cursor, in particular its class.

Step 110 determines if the class of the window under the cursor corresponds to a window class stored in the smart card 5. If not, the graphical representation of the cursor 9 is modified in step 11 1 to advise the user that at this stage the function for entering the password PWD is inhibited, i.e. that releasing the left-hand mouse button 6a will have no effect. The next step of the subroutine is then the end step 112. However, the Figure 4 subroutine is repeated for as long as the mouse 6 is moving, as is clear from the Figure 3 flowchart.

If the result of the test in step 110 is positive, i.e. if the window under the cursor is of a class contained in the memory of the smart card 5, step 113 modifies the graphical appearance of the cursor (which reverts to the arrow shape that it has when it reaches the window 8 in Figure 2), advising the user that insertion of the password PWD is then authorized.

If the event detected in step 102 in Figure 3 is releasing the left-hand mouse button, the subroutine 104 shown by the Figure 5 flowchart is executed.

Step 114 in Figure 5 corresponds to detecting release of the left-hand mouse button. The position of the mouse is acquired in step 115 and the window under the cursor is sought in step 116. Characteristic data of that window, in particular its class, is acquired in step 117.

Step 118 applies a test to determine if the window under the cursor 9 belongs to a class stored in the smart card 5. If not, the subroutine terminates in step 119.

If it does, the application to which the window belongs is determined in step 120. Step 121 applies a test to determine if the identified application corresponds to an application whose identification data is contained in the smart card 5. If it does, the password in the smart card 5 associated with the identified application is inserted in the window in which the cursor is then located, after which the subroutine terminates in step 123.

If the result of the test in step 121 is negative, the user is prompted in step 124 to enter the required password (static password) manually via the keyboard of their personal computer. In step 125 the password, the application identification data and the characteristics of the detected window acquired in steps 117 and 120 are transmitted to the smart card 5, which stores them. The next step of the subroutine is then step 122 which inserts the password entered at the keyboard by the user and stored in the smart card 5 into the destination window.”).

As Per Claim 36: The rejection of claim 35 is incorporated and further Freedman teaches:

- the GINA includes the random password generator, means for sending the newly generated password to the operating system for authentication, means for temporarily storing the new password and means for causing the new password to be stored in the secure media on verification by the operating system

(Column 12 Line 17 - Column 13 Line 37, as seen in the rejection of claim 35)

(Column 1, Lines 17-19, “If the password used is a static password it can be strong, i.e. long and complex (for example a series of random characters), which in practice is not possible with the conventional solution requiring the user to memorize it.”).

As Per Claim 37: The rejection of claim 29 is incorporated and further Claim 37 is substantially a restatement of the method of claim 15 as an apparatus and is rejected under substantially the same reasoning.

As Per Claim 38: The rejection of claim 37 is incorporated and further Claim 38 is substantially a restatement of the method of claim 16 as an apparatus and is rejected under substantially the same reasoning.

As Per Claim 39: The rejection of claim 37 is incorporated and further Claim 39 is substantially a restatement of the method of claim 17 as an apparatus and is rejected under substantially the same reasoning.

As Per Claim 40: The rejection of claim 39 is incorporated and further Claim 40 is substantially a restatement of the method of claim 18 as an apparatus and is rejected under substantially the same reasoning.

As Per Claim 41: The rejection of claim 37 is incorporated and further Claim 41 is substantially a restatement of the method of claim 19 as an apparatus and is rejected under substantially the same reasoning.

As Per Claim 42: The rejection of claim 41 is incorporated and further Claim 42 is substantially a restatement of the method of claim 20 as an apparatus and is rejected under substantially the same reasoning.

As Per Claim 43: The rejection of claim 42 is incorporated and further Claim 43 is substantially a restatement of the method of claim 21 as an apparatus and is rejected under substantially the same reasoning.

As Per Claim 44: The rejection of claim 37 is incorporated and further Claim 44 is substantially a restatement of the method of claim 26 as an apparatus and is rejected under substantially the same reasoning.

As Per Claim 45: The rejection of Claim 29 is incorporated and further Freedman teaches:

- A computer including apparatus according to claim 29 for authenticating a user to the computer of an application running on the computer

(Column 1, Lines 6-14, "Access to many computer programs, such as operating systems and application programs, for example for electronic mail, e-commerce, home banking, etc, requires authentication of the user vis-à-vis the program concerned. When a user starts a program requiring authentication on a terminal such as a personal computer, the program generally displays on the screen of the terminal a dialog box including two fields, one for entering the login name of the user and the other for entering their password. These credentials are specific to the user and to the program concerned and the user enters them via the keyboard of the terminal.").

As Per Claim 46: The rejection of Claim 29 is incorporated and further Freedman teaches:

- A computer network including apparatus according to claim 29 for authenticating a user to the network or to an application running on the network

(Column 1, Lines 6-14, “Access to many computer programs, such as operating systems and application programs, for example for electronic mail, e-commerce, home banking, etc, requires authentication of the user vis-à-vis the program concerned. When a user starts a program requiring authentication on a terminal such as a personal computer, the program generally displays on the screen of the terminal a dialog box including two fields, one for entering the login name of the user and the other for entering their password. These credentials are specific to the user and to the program concerned and the user enters them via the keyboard of the terminal.”).

As Per Claim 47: Claim 47 is substantially a restatement of the method of claim 1 as an apparatus and is rejected under substantially the same reasoning.

As Per Claim 49: Claim 49 is substantially a restatement of the method of claim 1 as an apparatus and is rejected under substantially the same reasoning.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 6-9, 13, 14, 33, 34, 48, 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freedman in view of Official Notice.

<u>**As Per Claims 6-9:**</u> The rejection of claim 1 is incorporated and further Freedman teaches:

- the password stored as part of the authentication credentials on the secure media without disclosing the new password to the user

- authenticating the new password and storing the new password on the secure media, when authenticated as part of the user's authentication credentials

(Column 5, Lines 31-34 “Thanks to this last feature in particular, the authentication process can be implemented without the user knowing their credentials, which significantly improves security because the user cannot inadvertently divulge the credentials.”).

(Column 5, Lines 31-34 “Thanks to this last feature in particular, the authentication process can be implemented without the user knowing their credentials, which significantly improves security because the user cannot inadvertently divulge the credentials.”).

Freedman Does not explicitly teach: changing the password, generating a random password in response to a change password request, or the password is changed in response to a request generated by the computer operating system or an application running on the computer or by the user.

However the examiner is giving official notice that these are all normal password changing operations that were well known in the art at the time of invention was made. It would be obvious to one of ordinary skill in the art at the time of invention was made to incorporate these sorts of password changes in to Freedman's method because having more complex passwords still does not remove the security problems of having passwords that do not change.

As Per Claims 13: The rejection of claim 12 is incorporated and further Freedman teaches:

- the password stored as part of the authentication credentials on the secure media without disclosing the new password to the user

- authenticating the new password and storing the new password on the secure media, when authenticated as part of the user's authentication credentials

(Column 5, Lines 31-34 “Thanks to this last feature in particular, the authentication process can be implemented without the user knowing their credentials, which significantly improves security because the user cannot inadvertently divulge the credentials.”).

(Column 5, Lines 31-34 “Thanks to this last feature in particular, the authentication process can be implemented without the user knowing their credentials, which significantly improves security because the user cannot inadvertently divulge the credentials.”).

- the password is sent by the GINA to the operating system logon procedure, and, when authenticated, the GINA causes the new random password to be stored in the secure media

(Column 12 Line 17 - Column 13 Line 37, “The following description with reference to Figures 3 to 6 covers a second embodiment in which the user does not need to select the appropriate password, because it is selected automatically by the access control program LPA.

Figure 3 shows the overall way in which the mouse 6 controls the access control program LPA. The process starts with step 100 in which the left-hand mouse button 6a is pressed when the cursor 9 is on top of the icon 7. Step 101 corresponds to capture of the status of the mouse and step 102 to waiting for events that can be generated by the mouse, for example moving the mouse or releasing the left-hand mouse button.

If the event detected is movement of the mouse, the next step is step 103 corresponding to the subroutine whose flowchart is shown in Figure 4.

If the event detected by the access control software concerns the left-hand mouse button, the next step is step 104 corresponding to the subroutine whose flowchart is shown in Figure 5. Step 105 is the last step of the main program.

The Figure 4 subroutine starts in step 106 with detection of movement of the mouse. In step 107 the position of the mouse is acquired. In step 108 the window under the cursor 9 is sought. Step 109 corresponds to the acquisition of characteristic data of the window under the cursor, in particular its class.

Step 110 determines if the class of the window under the cursor corresponds to a window class stored in the smart card 5. If not, the graphical representation of the cursor 9 is modified in step 11 1 to advise the user that at this stage the function for entering the password PWD is inhibited, i.e. that releasing the left-hand mouse button 6a will have no effect. The next step of the subroutine is then the end step 112. However, the Figure 4 subroutine is repeated for as long as the mouse 6 is moving, as is clear from the Figure 3 flowchart.

If the result of the test in step 110 is positive, i.e. if the window under the cursor is of a class contained in the memory of the smart card 5, step 113 modifies the graphical appearance of the cursor (which reverts to the arrow shape that it has when it reaches the window 8 in Figure 2), advising the user that insertion of the password PWD is then authorized.

If the event detected in step 102 in Figure 3 is releasing the left-hand mouse button, the subroutine 104 shown by the Figure 5 flowchart is executed.

Step 114 in Figure 5 corresponds to detecting release of the left-hand mouse button. The position of the mouse is acquired in step 115 and the window under the cursor is sought in step 116. Characteristic data of that window, in particular its class, is acquired in step 117.

Step 118 applies a test to determine if the window under the cursor 9 belongs to a class stored in the smart card 5. If not, the subroutine terminates in step 119.

If it does, the application to which the window belongs is determined in step 120. Step 121 applies a test to determine if the identified application corresponds to an application whose identification data is contained in the smart card 5. If it does, the password in the smart card 5 associated with the identified application is inserted in the window in which the cursor is then located, after which the subroutine terminates in step 123.

If the result of the test in step 121 is negative, the user is prompted in step 124 to enter the required password (static password) manually via the keyboard of their personal computer. In step 125 the password, the application identification data and the characteristics of the detected window acquired in steps 117 and 120 are transmitted to the smart card 5, which stores them. The next step of the subroutine is then step 122 which inserts the password entered at the keyboard by the user and stored in the smart card 5 into the destination window.").

Freedman Does not explicitly teach: changing the password, the GINA generating a random password in response to a change password request.

However the examiner is giving official notice that these are all normal password changing operations that were well known in the art at the time of invention was made. It would be obvious to one of ordinary skill in the art at the time of invention was made to incorporate these sorts of password changes in to Freedman's method because having more complex passwords still does not remove the security problems of having passwords that do not change.

As per Claim 14: the limitations of claim 14 are redundant to the limitations already present in claim 13.

As Per Claims 33-34: The rejection of claim 29 is incorporated and further Freedman teaches:

- the password stored as part of the authentication credentials on the secure media without disclosing the new password to the user

- authenticating the new password and storing the new password on the secure media, when authenticated as part of the user's authentication credentials

(Column 5, Lines 31-34 "Thanks to this last feature in particular, the authentication process can be implemented without the user knowing their credentials, which significantly improves security because the user cannot inadvertently divulge the credentials.”).

(Column 5, Lines 31-34 “Thanks to this last feature in particular, the authentication process can be implemented without the user knowing their credentials, which significantly improves security because the user cannot inadvertently divulge the credentials.”).

Freedman Does not explicitly teach: generating a random password in response to a change password request

However the examiner is giving official notice that these are normal password changing operations that were well know in the art at the time of invention was made. It would be obvious to one of ordinary skill in the art at the time of invention was made to incorporate these sorts of password changes in to Freedman's method because having more complex passwords still does not remove the security problems of having passwords that do not change.

As Per Claims 48: The rejection of claim 47 is incorporated and further Claim 48 is substantially a restatement of the method of claim 13 as an apparatus and is rejected under substantially the same reasoning.

<u>As Per Claims 50:</u> The rejection of claim 49 is incorporated and further Claim 50 is substantially a restatement of the method of claim 13 as an apparatus and is rejected under substantially the same reasoning.

10. Claims 10, 11, 23 & 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Freedman in view of United States Patent Application Publication US 2002/0023057 A1 (Goodwin et al.).

<u>As Per Claim 10:</u> The rejection of claim 1 is incorporated and further Freedman does not explicitly teach the following limitation however Goodwin et al. in analogous art does teach the following limitation:

- running a password recovery process if the authentication credentials are not verified, the password recovery process comprising assigning a one-time password to the user, submitting the authentication credentials including the assigned one time password, authenticating the user, generating a change password request, generating a new password in response to the change password request, and updating the secure media with the new password

(Goodwin et al., Paragraph [0177], Lines 15-23, “A password recovery function allows a user to get a new password in the event that it is forgotten. This process does not require the user to interface with Customer Service. This process relies upon the secret code or key word phrase that the user provided in Service Screen #4 of the

Getting Started (at the end of the Getting Started wizard, this keyword is uploaded to the server and stored as part of the user's personal profile).").

(Goodwin et al., Paragraph [0179], Lines 1-8, "Once the user gets the temporary password, the user uses it to log in as normal. Once the server verifies that the password is valid, an additional check is made to determine whether the password that is provided is a temporary or long term password. If the password is a temporary password, then the client software launches the change password dialog box, and does not allow the box to be closed until the user enters the old password and a new one.").

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Goodwin et al. in to the teachings of Freedman, because one of ordinary skill in the art would be motivated to have a means for dealing with a lost password.

As Per Claim 11: The rejection of Claim 10 is incorporated and further Freedman teaches:

- the new password is a random password

(Column 1, Lines 17-19, "If the password used is a static password it can be strong, i.e. long and complex (for example a series of random characters), which in practice is not possible with the conventional solution requiring the user to memorize it.").

As Per Claim 23: The rejection of Claim 15 is incorporated and further Freedman teaches:

- **generating a new random password**

(Column 1, Lines 17-19, "If the password used is a static password it can be strong, i.e. long and complex (for example a series of random characters), which in practice is not possible with the conventional solution requiring the user to memorize it.").

- **on detection of completion of the password change storing the new password at the secure media**

(Column 13, Lines 32-35, "In step 125 the password, the application identification data and the characteristics of the detected window acquired in steps 117 and 120 are transmitted to the smart card 5, which stores them").

Freedman does not explicitly teach the following limitation however Goodwin et al. in analogous art does teach the following limitation:

- **detecting a password change screen relating to the application, submitting the new password to the application**

(Goodwin et al., Paragraph [0179], Lines 1-8, "Once the user gets the temporary password, the user uses it to log in as normal. Once the server verifies that the password is valid, an additional check is made to determine whether the password that is provided is a temporary or long term password. If the password is a temporary password, then the client software launches the change password dialog box, and does not allow the box to be closed until the user enters the old password and a new one.”).

It would have been obvious to one of ordinary skill in the art at the time of invention was made to incorporate the teachings of Goodwin et al. in to the teachings of Freedman, because one of ordinary skill in the art would be motivated to be able to change passwords as while a more complex password is more secure than a simple one it does not remove the security weakness of a password that is never changed.

As Per Claim 24: The rejection of claim 23 is incorporated and (Goodwin et al. Paragraph [0179], Lines 1-8, as seen in the rejection of claim 23) has already taught the limitations of claim 24.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN A. KAPLAN whose telephone number is (571)270-3170. The examiner can normally be reached on 7:30 a.m. - 5:00 p.m. E.S.T..

If attempts to reach the examiner by telephone are unsuccessful, the examiner’s supervisor, Kristine Kincaid can be reached on 571-272-4063. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Benjamin Kaplan

/Kristine Kincaid/
Supervisory Patent Examiner, Art Unit 2139